COMPUTING THE DEGREE OF THE FIELD OF N-TORSION POINTS

ADAM VAN TUYL

ABSTRACT. Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$, and $n \neq \text{char}(K)$ a prime. Then the field of n-torsion points is constructed by adjoining the coordinates of all the n-torsion points to K. In this paper we present an algorithm to calculate the degree of the resulting extension when $\text{char}(K) \neq 2, 3$ and n an odd prime. The algorithm is based upon the characteristic polynomial of the Frobenius endomorphism and the division polynomials of E. As an application, we use our algorithm to count the number of rational points on the modular curve $X(n)/\mathbb{F}_q$ when $q \equiv 1 \pmod{n}$.

1. INTRODUCTION

Let E be an elliptic curve over a field K, $\text{char}(K) \neq 2, 3$, given in the Weierstrass form $E : y^2 = x^3 + ax + b$. If F is any field extension of K, then the set of F-rational points of E, denoted $E(F)$, is the set of points

$$E(F) := \left\{(x, y) \in F^2 \;\middle|\; y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\}$$

where $\mathcal{O}$ denotes the point at infinity. An additive group structure can be imposed on $E(F)$ via the well known chord and tangent method with $\mathcal{O}$ being the identity element of $E(F)$. A point $P \in E(F)$ is called an *n-torsion point* if $\underbrace{P + \cdots + P}_{n} = nP = \mathcal{O}$. Fix an algebraic closure of K, say $\overline{K}$, and let $E[n]$ denote the set of all n-torsion points in $E(\overline{K})$. We define $F = K_{E,n}$, the *field of n-torsion points of E*, to be the smallest subfield of $\overline{K}$ such that $E[n] \subset E(F)$.

The fields $K_{E,n}$ have appeared in questions related to class field theory (cf. [7]). The Galois representations of these fields also played an important role in the proof of Fermat's Last Theorem. Roughly speaking, the basis of this proof is to show that certain Galois extensions K of $\mathbb{Q}$ cannot be of the form $K = K_{E,n}$, thereby leading to the non-existence of a solution. Wiles (cf. [13]) gives a precise overview of which Galois extensions $K/\mathbb{Q}$ can be of the form $K_{E,n}$ for an elliptic curve $E/\mathbb{Q}$.

In this paper we study the case when $\mathbb{Q}$ is replaced by $K = \mathbb{F}_q$. In this case $K_{E,n}$ is completely determined by its degree $d = [K_{E,n} : K]$. The main result of this paper is to present an algorithm to calculate d when $\text{char}(K) \neq 2, 3$ and n is an odd prime distinct from $\text{char}(K)$. Although our algorithm is admittedly simple in that it requires only basic properties about elliptic curves over finite fields, to our knowledge there is no other reference for a method for calculating d. We also give an application of our algorithm to compute $\#X(n)/\mathbb{F}_q$ when $q \equiv 1 \pmod{n}$.

1991 *Mathematics Subject Classification.* 11G25,11Y99.

Key words and phrases. n-torsion points, division polynomials, Frobenius endomorphism.

Our algorithm is based upon the fact that $K_{E,n}$ is a Galois extension of K, and thus, there exists an injective group homomorphism $\rho_n : \mathrm{Gal}(K_{E,n}/K) \hookrightarrow GL_2(\mathbb{Z}/n\mathbb{Z})$. Then, since the the Frobenius automorphism $\sigma_q \in \mathrm{Gal}(K_{E,n}/K)$ generates this Galois group, we use the fact that the characteristic polynomial of $\rho_n(\sigma_q)$ is $T^2 - a_E T + q \equiv 0 \pmod{n}$ where $a_E = (q+1) - \#E(\mathbb{F}_q)$ to demonstrate that in most cases the degree d can be found using basic linear algebra. Only in the case where the discriminant of the above equation is divisible by n do we need to invoke the use of the division polynomials of E.

We restrict ourselves to the case that $\mathrm{char}(K) \neq 2, 3$ in order to utilize the Weierstrass form of E and to utilize the division polynomials ψ_n described in Section 4. We also restrict to the case that n is an odd prime. If $n = 2$, then d is simply the degree of the splitting field for $E : y^2 = x^3 + ax + b$.

Our presentation is as follows. Section 2 introduces the extension $K_{E,n}$ and describes some its properties. Section 3 presents the characteristic polynomial of the Frobenius endomorphism and provides a partial solution to our problem. Section 4 describes the division polynomials of E and how they also give a partial solution. In the fifth section, we present our algorithm, and we discuss its implementation. In the sixth section, we discuss the problem of computing the degree of $K_{E,n}$ for all curves E over $\mathbb{F}_q$. In the final section, we demonstrate how one can use our algorithm to compute $\#X(n)(\mathbb{F}_q)$ when $q \equiv 1 \pmod{n}$.

The author would like to thank Satya Mohit and Srinath Baba for their comments. The author would especially like to thank Ernst Kani for introducing this problem to him and for his many helpful conversations and discussions.

2. The Field of N-Torsion Points

Let $K = \mathbb{F}_q$ be a finite field with $\mathrm{char}(K) \neq 2, 3$. Then an equation for an elliptic curve E over this field is given by the Weierstrass form $E : y^2 = x^3 + ax + b$. Furthermore, let $n \geq 3$ be a prime such that $n \neq \mathrm{char}(K)$. The goal of this section is to present some results, with a reference to their proofs, about $K_{E,n}$ that form the basis of our algorithm.

We begin by describing the group structure of $E[n]$.

Theorem 2.1 ([11] III.6.2)**.** *$E[n]$ is a finite subgroup of $E(\overline{K})$ of order n^2, and*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Notice that for all n, $\mathcal{O} \in E[n]$. Using Theorem 2.1, we can write $E[n]$ as

$$E[n] = \{\mathcal{O}, (x_1, y_1), \ldots, (x_m, y_m)\},$$

where $m = n^2 - 1$. Taking the coordinates $\{x_i, y_i\}$ for every $1 \leq i \leq m$, and adjoining them to our base field K, we construct the field of n-torsion points $K_{E,n}$. Explicitly,

$$K_{E,n} := K(E[n]) = K(x_1, y_1, \ldots, x_m, y_m).$$

It is clear that the degree d of the extension of $K_{E,n}$ is finite.

Remark 2.2. Let ζ_n denote an n^{th} root of unity of $\overline{K}$. By the Weil pairing, $\zeta_n \in K_{E,n}$ ([11] III.6.8). Since $K_{E,n} = \mathbb{F}_{q^d}$, then $\zeta_n \in K_{E,n}$ implies that $n = \mathrm{ord}(\zeta_n) | q^d - 1$. So, $q^d \equiv 1 \pmod{n}$, or equivalently, $\mathrm{ord}(q, n) | d$, where $\mathrm{ord}(q, n)$ is the order of q in $(\mathbb{Z}/n\mathbb{Z})^\times$.

The field $K_{E,n}$ is a Galois extension of its base field K. For any Galois extension K' of K, an element $\sigma \in \mathrm{Gal}(K'/K)$ induces a map on the K'-rational points of E. Moreover, since the group structure is defined over K, the Galois action is linear. From these facts we obtain the well known Galois representation of $\mathrm{Gal}(K_{E,n}/K)$.

Theorem 2.3. *Let E be an elliptic curve over K and $n \geq 2$ be an prime $\neq \mathrm{char}(K)$. Then there is an injective group homomorphism*

$$\rho_n : \mathrm{Gal}(K_{E,n}/K) \hookrightarrow GL_2(\mathbb{Z}/n\mathbb{Z})$$

defined with respect to a basis for $E[n]$.

Computing d, therefore, is equivalent to finding the cardinality of the image of ρ_n in $GL_2(\mathbb{Z}/n\mathbb{Z})$. We can recover more information about d by recalling that K is a finite field. If K' is any Galois extension of K, then $\mathrm{Gal}(K'/K)$ is a cyclic group and the *Frobenius automorphism* $\sigma_q \in \mathrm{Gal}(K'/K)$ generates the Galois group, where $\sigma_q : K' \to K'$ is defined by $x \mapsto x^q$. From this fact, we now have:

Corollary 2.4. *Let $\sigma_q \in \mathrm{Gal}(K_{E,n}/K)$ be the Frobenius automorphism. Then $d = \mathrm{ord}(\rho_n(\sigma_q))$ in $GL_2(\mathbb{Z}/n\mathbb{Z})$.*

Proof. Because ρ_n is injective, $|\mathrm{Im}(\rho_n)| = \mathrm{ord}(\rho_n(\sigma_q))$ in $GL_2(\mathbb{Z}/n\mathbb{Z})$. □

We show below that we can determine the characteristic polynomial of the matrix $\rho_n(\sigma_q)$ from the elliptic curve E. From this information, we can calculate the order of $\rho_n(\sigma_q) \in GL_2(\mathbb{Z}/n\mathbb{Z})$ for a fixed E and almost all n.

3. The Characteristic Polynomial of the Frobenius Endomorphism

Let E be an elliptic curve over K and let $\phi_q \in \mathrm{End}(E)$ be the *Frobenius Endomorphism* defined by

$$(\phi_q)(P) = \begin{cases} (x^q, y^q) & \text{if } P = (x,y) \in E(\overline{K}) \text{ and } P \neq \mathcal{O} \\ \mathcal{O} & \text{if } P = \mathcal{O} \end{cases}.$$

Then the characteristic polynomial of ϕ_q in $\mathrm{End}(E)$ is

$$f(T) = T^2 - a_E T + q,$$

where $a_E := (q+1) - \#E(\mathbb{F}_q)$ [12]. Restricting ϕ_q to $E[n]$ induces an element $\phi_q|_{E[n]} \in \mathrm{Aut}(E[n])$ whose characteristic polynomial is congruent modulo n to $f(T)$.

Let $\sigma_q \in \mathrm{Gal}(K_{E,n}/K)$ be the Frobenius automorphism. Then the induced endomorphism on E is given by the map

$$(\sigma_q)_E(P) = \begin{cases} (\sigma_q(x), \sigma_q(y)) = (x^q, y^q) & \text{if } P = (x,y) \in E(\overline{K}) \text{ and } P \neq \mathcal{O} \\ \mathcal{O} & \text{if } P = \mathcal{O} \end{cases}.$$

Restricting $(\sigma_q)_E$ to $E[n]$, we note that $(\sigma_q)_E|_{E[n]} = \phi_q|_{E[n]}$. Moreover, $(\sigma_q)_E|_{E[n]}$ is identified with $\rho_n(\sigma_q)$ in $GL_2(\mathbb{Z}/n\mathbb{Z})$ via the Galois representation. But now $(\sigma_q)_E|_{E[n]} \in \mathrm{Aut}(E[n])$, and since $\mathrm{Aut}(E[n]) \xrightarrow{\sim} GL_2(\mathbb{Z}/n\mathbb{Z})$ once we pick a basis, the characteristic polynomial of $\rho_n(\sigma_q)$ will be the same as the characteristic polynomial of $(\sigma_q)_E|_{E[n]}$ in $\mathrm{Aut}(E[n])$. In particular, we have

Theorem 3.1. *The polynomial*

$$f(T) = T^2 - a_E T + q$$

is congruent modulo n to the characteristic polynomial of $\rho_n(\sigma_q) \in GL_2(\mathbb{Z}/n\mathbb{Z})$.

From the characteristic polynomial, we can calculate d in a large number of cases.

Theorem 3.2. *Let E be an elliptic curve over the field $K = \mathbb{F}_q$, where, $\mathrm{char}(K) \neq 2, 3$ and n an odd prime $\neq \mathrm{char}(K)$. Let $ch_{\rho_n(\sigma_q)}(T) \equiv T^2 - a_E T + q \pmod{n}$ be the characteristic polynomial of $\rho_n(\sigma_q)$. Suppose that $ch_{\rho_n(\sigma_q)}$ factors over $\overline{\mathbb{F}}_n$ as*

$$ch_{\rho_n(\sigma_q)}(T) = (T - \alpha)(T - \beta).$$

Let $c = \left(\frac{a_E^2 - 4q}{n}\right)$, where $\left(\frac{}{n}\right)$ is the Legendre symbol. Then,

- *(i) if $c = 1$, then $\alpha, \beta \in \mathbb{F}_n$ and $d = \mathrm{lcm}(\mathrm{ord}(\alpha, n), \mathrm{ord}(\beta, n))$, where $\mathrm{ord}(t, n) :=$ the order of t in $\mathbb{F}_n^\times$;*
- *(ii) if $c = -1$, then $\alpha, \beta \in \mathbb{F}_{n^2} \backslash \mathbb{F}_n$, $\beta = \alpha^n$, and d is equal to the order of $\alpha \in \mathbb{F}_{n^2}^\times$;*
- *(iii) if $c = 0$, then $\alpha = \beta \in \mathbb{F}_n$ and $d = \mathrm{ord}(\alpha, n)$ or $d = n\,\mathrm{ord}(\alpha, n)$.*
- *(iv) if $n > 4q$ or $\left(\frac{q}{n}\right) = -1$, then $c \neq 0$, in which case we can determine d explicitly.*

Proof. Fix once and for all a basis for $GL_2(\mathbb{Z}/n\mathbb{Z})$. Observe that $a_E^2 - 4q$ is the discriminant of the characteristic polynomial. So, if $c = 1$, then (i) follows from the fact that then $ch_{\rho_n(\sigma_q)}$ factors in $\mathbb{F}_n$ and has two distinct roots, α and β, in this field. Furthermore, α and β are the eigenvalues of the matrix $\rho_n(\sigma_q)$. Thus,

$$\rho_n(\sigma_q) \sim \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix},$$

with respect to our basis. Hence, the order of $\rho_n(\sigma_q)$ is equal to $\mathrm{lcm}(\mathrm{ord}(\alpha, n), \mathrm{ord}(\beta, n))$.

For (ii), $\alpha, \beta \in \mathbb{F}_{n^2}$ since they are roots of $ch_{\rho_n(\sigma_q)}(T)$, a monic irreducible polynomial of degree 2 in $\mathbb{F}_q[T]$. Moreover, since β is a conjugate of α, we can write it as $\beta = \alpha^n$ since σ_n generates $\mathrm{Gal}(\mathbb{F}_{n^2}/\mathbb{F}_n)$. Thus

$$\rho_n(\sigma_q) \sim \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^n \end{pmatrix}.$$

But then it is clear that the order of $\rho_n(\sigma_q)$ is equal to the order of α in $\mathbb{F}_{n^2}^\times$.

If (iii) holds, then there is only one eigenvalue, i.e. $\alpha = \beta \in \mathbb{F}_n$. But then, by the Jordan Canonical Form,

$$\rho_n(\sigma_q) \sim \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \quad \text{or} \quad \rho_n(\sigma_q) \sim \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix},$$

depending upon the dimension of the eigenspace. If $\rho_n(\sigma_q)$ is diagonal, then the order of $\rho_n(\sigma_q)$ is the order of α in $\mathbb{F}_n$. However, suppose that the other case occurs. We observe that $\rho_n(\sigma_q)^t \sim \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}^t = \begin{pmatrix} \alpha^t & t\alpha^{t-1} \\ 0 & \alpha^t \end{pmatrix}$ for all $t \in \mathbb{Z}$. Letting $t = n$, we find that $\rho_n(\sigma_q)^t$ is a diagonal matrix with α's along the diagonal since $\rho_n(\sigma_q) \in GL_2(\mathbb{Z}/n\mathbb{Z})$. Thus, the order of $\rho_n(\sigma_q)$ must be $n\mathrm{ord}(\alpha, n)$.

Finally, we have $|a_E| \leq 2\sqrt{q}$ (see [11] V.1.1) . If $n > 4q$, then $n > |a_E^2 - 4q|$, from which it is clear that $\left(\frac{a_E^2 - 4q}{n}\right) \neq 0$. Assuming that $\left(\frac{q}{n}\right) = -1$, then $c \neq 0$ since $c = 0$ implies $\left(\frac{q}{n}\right) = 1$. Thus (iv) holds. □

Corollary 3.3. *Let E be an elliptic curve over K and let $d = [K_{E,n} : K]$, where, as before, $n \neq \mathrm{char}(K)$. If $c = \left(\frac{a_E^2-4q}{n}\right)$, then we have the following relations between d and n:*

(*i*) *if $c = 1$, then $d|(n-1)$.*
(*ii*) *if $c = 0$, then $d|n(n-1)$.*
(*iii*) *if $c = -1$, then $d|\,\mathrm{ord}(q,n)(n+1)$ and $\mathrm{ord}(q,n)(n+1)|n^2-1$.*
(*iv*) *$\mathrm{ord}(q,n)|d$ always holds.*

Proof. The first two assertions follow from Theorem 3.2 since $\mathrm{ord}(\alpha,n)|n-1$ for all $\alpha \in \mathbb{F}_n$. The last assertion was noted in Remark 2.2.

For statement (*iii*), we note that since $\left(\frac{a_E^2-4q}{n}\right) = -1$, d is equal to the order of $\alpha \in \mathbb{F}_{n^2}$, where α is one of the roots of the characteristic polynomial. Let g be a generator of $\mathbb{F}_{n^2}^{\times}$. So, $\alpha = g^t$ for some $t \in \mathbb{Z}$. Moreover, from Theorem 3.1 we have $\alpha\alpha^n = q \in \mathbb{F}_{n^2}$. Let $b = \mathrm{ord}(q,n)$. Then $(g^t)^{(1+n)b} = \alpha^{(1+n)b} = (\alpha^{(1+n)})^b = q^b = 1$. Since d is the order of g^t, we have $d|\,\mathrm{ord}(q,n)(n+1)$. □

In Theorem 3.2 the value of a_E does not determine d completely in the case $c = 0$. However, in many cases, the following criterion allows us to determine d.

Proposition 3.4. *Let E be an elliptic curve over K and let*

$$f(T) = T^2 - a_E T + q = (T-\delta)(T-\gamma)$$

be the factorization of $f(T)$ in $\overline{\mathbb{Q}}[T]$. Suppose that $a_E^2 - 4q \equiv 0 \pmod{n}$, and so, $f(T)$ has a repeated root α modulo n. Set $d^* = ord(\alpha, n)$. If $n^2 \nmid 1+q^{d^*}-(\delta^{d^*}+\gamma^{d^*})$, then $d = [K_{E,n} : K] = nd^*$.

Proof. We know from Theorem 3.2 that $d = d^*$ or $d = nd^*$. Suppose that $d = d^*$. Since $E[n]$ is a subgroup of $E(\mathbb{F}_{q^{d^*}})$, we must have $n^2|\#E(\mathbb{F}_{q^{d^*}})$. However, from [11] V.2.4, we know that $\#E(\mathbb{F}_{q^{d^*}}) = (1+q^{d^*}) - (\delta^{d^*}+\gamma^{d^*})$. This contradicts our assumption that $n^2 \nmid (1+q^{d^*}) - (\delta^{d^*}+\gamma^{d^*})$. □

Remark 3.5. In Example 5.4 we will show that the converse is false.

4. The Division Polynomials of an Elliptic Curve

Following [9], we introduce the *division polynomials* $\tilde{\psi}_n \in K[x,y]$ which are defined inductively as follows:

$$\begin{aligned}
\tilde{\psi}_{-1} &= -1, \quad \tilde{\psi}_0 = 0, \quad \tilde{\psi}_1 = 1, \quad \tilde{\psi}_2 = 2y \\
\tilde{\psi}_3 &= 3x^4 + 6ax^2 + 12bx - a^2 \\
\tilde{\psi}_4 &= 4y(x^6 - 5ax^4 + 20bx^3 - 5ax^2 - 4abx - 8b^2 - a^3) \\
\tilde{\psi}_n = \tilde{\psi}_{2m+1} &= \tilde{\psi}_{m+2}\tilde{\psi}_m^3 - \tilde{\psi}_{m-1}\tilde{\psi}_{m+1}^3, \qquad m \geq 2 \\
2y\tilde{\psi}_n = 2y\tilde{\psi}_{2m} &= \tilde{\psi}_m(\tilde{\psi}_{m+2}\tilde{\psi}_{m-1}^2 - \tilde{\psi}_{m-2}\tilde{\psi}_{m+1}^2), \qquad m \geq 3,
\end{aligned}$$

where $a, b \in K$. Via induction on n, one can show that $\tilde{\psi}_n$ is a polynomial.

We define the polynomials $\psi_n \in K[x]$, which we call the n^{th} *division polynomial of* E, as follows. We eliminate all y^2-terms from $\tilde{\psi}_n$ by using the relation $E : y^2 = x^3 + ax + b$. The resulting polynomial $\tilde{\psi}'_n(x,y)$ is either in $K[x]$ if n is odd or in $yK[x]$ if n is even. We define $\psi_n(x) = \tilde{\psi}'_n(x,y)$ if n is odd, $\psi_n(x) = \tilde{\psi}'_n(x,y)/y$ if n

is even. By induction on n, one can describe the behavior of ψ_n^2 as a polynomial in $K[x]$. In fact, one finds that for n odd

$$\psi_n^2(x) \quad = \quad n^2 x^{n^2-1} + \text{ lower order terms.}$$

The following proposition, which can be found in [8], connects the root of the n^{th}-division polynomial of E with the x-coordinate of an n-torsion point.

Proposition 4.1. *If $P = (x(P), y(P)) \in E(\overline{K})\backslash\{\mathcal{O}\}$, with $P \notin E[2]$, then*

$$[n]P = \mathcal{O} \quad \text{if and only if} \quad \psi_n(x(P)) = 0.$$

From the division polynomial ψ_n we can find the x-coordinates of the n-torsion points. Supposing that n is odd, then ψ_n is a polynomial in x. If we suppose that $K = \mathbb{F}_q$ and factor ψ_n over $\mathbb{F}_q[x]$, we get $\psi_n = f_1 \cdots f_r$ where each f_i is irreducible in $\mathbb{F}_q[x]$. We also notice that the f_i's are distinct. Indeed, let $x_i \in \overline{\mathbb{F}_q}$ be a root of ψ_n. Then to x_i we can associate two n-torsion points, namely, $P_{i1} = (x_i, \sqrt{x_i^3 + ax_i + b})$ and $P_{i2} = (x_i, -\sqrt{x_i^3 + ax_i + b})$. The expression in the square root is not zero since that would imply that $P_{i1} = P_{i2}$ is a 2-torsion point. Since ψ_n has degree $\frac{n^2-1}{2}$, it can have at most $\frac{n^2-1}{2}$ distinct roots. But because there are $n^2 - 1$ torsion points besides the point at infinity, each root of ψ_n must be distinct.

We show how to determine d up to a factor of 2 from the way ψ_n factors in $\mathbb{F}_q[x]$.

Theorem 4.2. *Let n be an odd prime, and let $K = \mathbb{F}_q$ with $n \neq \text{char}(K)$. Suppose that ψ_n factors in $K[x]$ as $\psi_n = f_1 \cdots f_r$. Set $d_i = \deg(f_i)$ and let $l := \text{lcm}(\{d_i\}_{i=1}^r)$. Let $K'_{E,n} = K(x_1, x_2, \ldots, x_{n^2-1})$, where the x_i's are the x-coordinates of the n-torsion points. Then $[K'_{E,n} : K] = l$. Furthermore, $[K_{E,n} : K'_{E,n}] = 1$ or 2; equivalently, $d = l$ or $d = 2l$.*

Proof. The field $K'_{E,n}$ is the splitting field of ψ_n over K. Since K is a finite field, $[K'_{E,n} : K]$ is equal to to the least common multiple of the degrees of ψ_n's irreducible factors over K.

To prove the second claim, suppose that $K_{E,n} \neq K'_{E,n}$. Then there exists some x_i such that $y_i = \sqrt{x_i^3 + ax_i + b} \notin K'_{E,n} = \mathbb{F}_{q^l}$. But then $K'_{E,n}(y_i) = \mathbb{F}_{q^{2l}}$, and every element of $x \in \mathbb{F}_{q^l}$ has a square root in $\mathbb{F}_{q^{2l}}$. In particular, all $y_i \in \mathbb{F}_{q^{2l}}$. Thus, in this case $[K_{E,n} : K'_{E,n}] = 2$. □

5. An Algorithm for Computing $[K_{E,n} : K]$ and its Implementation

So far we have presented only partial solutions (Theorems 3.2 and 4.2) to the problem of calculating $d = [K_{E,n} : K]$. In this section we introduce an algorithm which combines these solutions. We assume that the following has been given:

(*i*) $q = p^r$, where $K = \mathbb{F}_q$, and $\text{char}(K) = p \neq 2, 3$.
(*ii*) n, a prime such that $n \neq \text{char}(K)$ and $n \geq 3$.
(*iii*) a and b, the coefficients of the elliptic curve E over K in Weierstrass form.

From Theorem 3.2, if we know a_E and if $\left(\frac{a_E^2 - 4q}{n}\right) \neq 0$, then we can calculate d. If $\left(\frac{a_E^2 - 4q}{n}\right) = 0$, then we know that $d = n\text{ord}(\alpha, n)$ or $\text{ord}(\alpha, n)$. By using the factorization of ψ_n in $K[x]$, we can distinguish between the two possibilities.

Lemma 5.1. *Suppose* $\left(\frac{a_E^2-4q}{n}\right) = 0$. *Let* $\psi_n = f_1 \cdots f_r$ *be the factorization of* ψ_n *into irreducible factors in* $K[x]$. *Set* $l = \operatorname{lcm}(\{\deg(f_i)\}_{i=1}^r)$ *and let* $d^* = \operatorname{ord}(\alpha, n)$. *Then*

$$d = [K_{E,n} : K] = \begin{cases} d^* & \text{if } d^* = l \text{ or } d^* = 2l \\ nd^* & \text{otherwise.} \end{cases}$$

Proof. From Theorem 4.2, we know that $d = l$ or $d = 2l$. Suppose that $d^* = l$. Then if $d = nd^*$, then $l \neq d$ and $2l \neq d$ since n is an odd prime. So, $d = d^*$. Similarly suppose that $d^* = 2l$. If $d = nd^*$, then $l \neq d$ and $2l \neq d$. So, $d = d^*$.

Now suppose that $d^* \neq l$ and $d^* \neq 2l$. Then $d \neq d^*$ since $d = l$ or $d = 2l$. So, $d = nd^*$. □

The above lemma is the final piece in our algorithm to compute d. We summarize below.

Algorithm 5.2. *Suppose that* $a, b, q,$ *and* n *have been given.*

1. *Compute* $a_E = (1+q) - \#E(\mathbb{F}_q)$ *by computing* $\#E(\mathbb{F}_q)$ *(See below)*
2. *Let* $c = \left(\frac{a_E^2-4q}{n}\right)$, *where* $\left(\frac{}{n}\right)$ *is the Legendre symbol.*
3. *If* $c = 1$, *then* $T^2 - a_E T + q \equiv (T-\alpha)(T-\beta) \pmod{n}$, *where* $\alpha \neq \beta \in \mathbb{F}_n$, *and*
   $d = \operatorname{lcm}(\operatorname{ord}(\alpha, n), \operatorname{ord}(\beta, n))$
   else if $c = -1$, *then* $T^2 - a_E T + q \equiv (x-\alpha)(x-\alpha^n) \in \mathbb{F}_{n^2}$, *and*
   $d =$ *order of* α *in* $\mathbb{F}_{n^2}^{\times}$.
   else if $c = 0$, *then* $T^2 - a_E T + q \equiv (T-\alpha)^2, \alpha \in \mathbb{F}_n$. *Then*
   1. $d^* = \operatorname{ord}(\alpha, n)$.
   2. $T^2 - a_E T + q = (T-\delta)(T-\gamma) \in \mathbb{C}[x]$.
   3. *If* $n^2 | (1+q^{d^*}) - (\delta^{d^*} - \gamma^{d^*})$ *then*
      1. *Construct* ψ_n *and factor* ψ_n *in* $\mathbb{F}_q[x]$.
      2. *Let* $l = \operatorname{lcm}(\{\deg(f_i)\}_{i=1}^r)$ *where* $\psi_n = f_1 \cdots f_r$.
      3. *if* $d^* = l$ *or* $d^* = 2l$ *then*
         $d = d^*$.
         else
         $d = nd^*$
      else
      $d = nd^*$

Remark 5.3. The number a_E is fundamental to the Algorithm 5.2. By definition, computing a_E is equivalent to computing $\#E(\mathbb{F}_q)$. However, computing the number of points on an elliptic curve over a finite field $K = \mathbb{F}_q$, even when $q = p$, is a non-trivial matter for large p. Since the appearance of Schoof's ground breaking paper [9] on this topic, much work has gone into this question. For a nice exposition on a variety of methods to compute $\#E(\mathbb{F}_p)$ one should consult [10],[2], and [4]. In [10], Schoof claims that for small primes a simple brute force method of counting points on the curve is efficient. For large primes a less naive method must be used. (In [10], a small prime is defined to be $p < 200$. However, faster computers have made this bound obsolete.) Hence, to use Algorithm 5.2 for large p, one will need to first implement an efficient algorithm for computing $\#E(\mathbb{F}_p)$.

Example 5.4. We give an example of two curves, E_1 and E_2, such that $a_E := a_{E_1} = a_{E_2}$, and $a_E^2 - 4q \equiv 0 \bmod n$, but the degrees of their field of n-torsion points differ by a factor of n.

Let $E_1 : y^2 = x^3 + 2$ and $E_2 : y^2 = x^3 + 6x + 2$ be two curves over $K = \mathbb{F}_7$. We wish to compute the degree d of the field of 3-torsion points. By counting the number of K-rational points on each curve, we find that $a_E := a_{E_1} = a_{E_2} = -1$. So, the characteristic polynomials are equal modulo n, specifically,

$$ch_{\rho(\sigma_q,E_1)}(T) \equiv ch_{\rho(\sigma_q,E_2)}(T) \equiv (T-1)^2 \pmod 3.$$

Both matrices have repeated eigenvalues since $\left(\frac{a_E^2-4q}{n}\right) = \left(\frac{-27}{3}\right) = 0$. So $\alpha \equiv 1 \pmod 3$, since $\alpha^2 \equiv q \pmod 3$ and $q \equiv 1 \pmod 3$. Since $\mathrm{ord}(\alpha, 3) = 1$, then $[K_{E_1,3} : K] = 1$ or 3 by Theorem 3.2. Similarly for $[K_{E_2,3} : K]$. Forming the 3-division polynomials for each curve and factoring over $\mathbb{F}_q[x]$, we get

$$\psi_{3,E_1} \equiv 3x^4 + 24x \equiv 3x(x+4)(x+2)(x+1) \pmod 7,$$

and

$$\psi_{3,E_2} \equiv 3x^4 + 36x^2 + 24x - 36 \equiv (x+1)(3x^3 + 4x^2 + 4x + 6) \pmod 7.$$

From this factorization, we deduce that $[K_{E_1,3} : K] = 1$, but $[K_{E_2,3} : K] = 3$.

We also point out that the curve $E_2 : y^2 = x^3 + 6x + 2$ is a counterexample to the converse of Proposition 3.4. In this case $n^2 \mid \#E(\mathbb{F}_{q^{d^*}})$ since $3^2 \mid (1 + 7 - a_E)$ with $d^* = 1$. However, $d \neq 1$, but $d = 3$, as we have just shown.

We now discuss some of the methods we used to implement our algorithm. As noted in Remark 5.3, the computation of a_E is integral to this algorithm. If one is interested in only small p (or small q), and if E is an elliptic curve over $\mathbb{F}_q$ given in Weierstrass form, i.e., $E : y^2 = x^3 + ax + b$, the following formula enables one to calculate a_E:

$$a_E = -\sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + ax + b}{\mathbb{F}_q}\right), \tag{1}$$

where $\left(\frac{}{\mathbb{F}_q}\right)$ is the quadratic character defined by

$$\left(\frac{x}{\mathbb{F}_q}\right) := \begin{cases} 1 & \text{if } \exists y \in \mathbb{F}_q \text{ such that } y^2 = x \\ -1 & \text{if } \nexists y \in \mathbb{F}_q \text{ such that } y^2 = x \\ 0 & \text{if } x = 0. \end{cases}$$

In the case that $q = p$, then the above is simply the Legendre symbol. Our implementation of Algorithm 5.2 to calculate the tables at the end of the paper made use of (1) to calculate a_E since we were concerned with primes $p < 100$.

In the case that $\left(\frac{a_E^2-4q}{n}\right) = -1$, it was shown in Theorem 3.2 that d is equal to the order of $\alpha \in \mathbb{F}_{n^2}$, where α is a root of $f(T) \equiv T^2 + a_E T + q \pmod n$. To calculate the order of α we need to construct $\mathbb{F}_{n^2}$ and identify α with an element in this field. To construct $\mathbb{F}_{n^2}$, we can use the fact that f is irreducible in the ring $\mathbb{F}_n[T]$. Hence $\mathbb{F}_{n^2} \cong \frac{\mathbb{F}_n[T]}{(f)}$. Since $f(\alpha) \equiv 0 \pmod n$ we have $T \equiv \alpha \pmod f$. So, we only need to discern the order of T in $\mathbb{F}_n[T]/(f)$.

Algorithm 5.2 also relies on ψ_n to distinguish between the two possible values for d in the case that $a_E^2 - 4q \equiv 0 \pmod n$. However, as n becomes large, the degree of ψ_n grows like $\frac{n^2-1}{2}$. This is unfortunate since this implies that as n increases, the algorithm slows down since we need to factor ψ_n. The natural question arises:

is there any fast alternative to factoring ψ_n to determine to determine d in the case that $a_E^2 - 4q \equiv 0 \pmod{n}$? This is a question that requires further attention.

6. Computing $[K_{E,n} : K]$ for all E over $\mathbb{F}_q$

In this section we discuss how to compute $d = [K_{E,n} : K]$ for all elliptic curves over a finite field. We first describe how to construct all the elliptic curves over a field K. Then we describe how to compute d for an elliptic curve E and its quadratic twist E' by computing d for only one of the two curves. For some motivation, see the next section.

Let E be an elliptic curve over $K = \mathbb{F}_q$ given in Weierstrass form, $E : y^2 = x^3 + ax + b$. We can associate with every curve E an invariant, called the *j-invariant*, where $j_E = 1728\frac{4a^3}{4a^3+27b^2}$. If we pick $j \in K$ such that $j \neq 0, 1728$, we can construct a curve E with this j-invariant, namely,

$$E_j : y^2 = x^3 - \frac{27j}{j-1728}x + \frac{54j}{j-1728}. \tag{2}$$

In fact, under the hypothesis that $j \neq 0, 1728$ and K is a finite field, then there are only *two* curves up to K-isomorphism over K with this j-invariant: the above curve and its quadratic twist,

$$E_{j,twist} : y^2 = x^3 - \frac{27j}{j-1728}g^2x + \frac{54j}{j-1728}g^3,$$

where g is not a square in K. See [11] X.5 for more on twisting.

We see from the formula for j_E that $j = 0$ if and only if $E : y^2 = x^3 + b$. Over K, there are always $k = |\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^6|$ such curves, and we have $k = 6$ if $q \equiv 1 \pmod 3$ and $k = 2$ if $q \not\equiv 1 \pmod 3$. If $q \equiv 1 \pmod 3$ these curves are $E : y^2 = x^3 + g$ where $g \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^6$. If $q \not\equiv 1 \pmod 3$, then there are only two curves, $E : y^2 = x^3 + 1$ and its quadratic twist $E' : y^2 = x^3 + g$, where g is not a square in $\mathbb{F}_q$. The case for $j = 1728$ is similar.

From the above, we can construct all curves E over K by running through all $j \in \mathbb{F}_q$ and find the coefficients of the curve with this j-invariant using (2), or in the case that $j = 0$ and $j = 1728$, $E : y^2 = x^3 + 1$ and $E : y^2 = x^3 + x$ respectively. Then, depending upon the q, we form the twists of the curves. This is the strategy we used in the appendix to find the coefficients of all the elliptic curves over K. We can then pass the coefficients onto our algorithm to compute d.

However, as we show below, we need only compute $d = [K_{E,n} : K]$ for one curve in the twist class if $j \neq 0, 1728$.

Lemma 6.1. *Let E be an elliptic curve over $K = \mathbb{F}_q$ with $j \neq 0, 1728$, and let E' denote the quadratic twist of E over K. Then $a_E = -a_{E'}$.*

Proof. Section III.3.1 of [2] gives a proof that $\#E(K) + \#E'(K) = 2q + 2$. The conclusion follows from using this identity and the definition of a_E and $a_{E'}$. □

Proposition 6.2. *Let E be an elliptic curve over $K = \mathbb{F}_q$ with $j \neq 0, 1728$. Let E' be the quadratic twist of E over K, and suppose that $n \neq \mathrm{char}(K)$ is prime. Let $d = [K_{E,n} : K]$ and $d' = [K_{E',n} : K]$. Then*

(i) if $2 \nmid d$, then $d' = 2d$.
(ii) if $4|d$, then $d' = d$.

(*iii*) *if* $2|d$ *but* $4 \nmid d$, *then*

$$d' = \begin{cases} \frac{d}{2} & \text{if } ord(q,n) \equiv 1 \pmod 2 \\ d & \text{if } ord(q,n) \equiv 0 \pmod 2 \end{cases}.$$

Proof. By Lemma 6.1, we have $a_E = -a_{E'}$. Let σ_E (resp. $\sigma_{E'}$) be the Frobenius automorphism that generates $\mathrm{Gal}(K_{E,n}/K)$ (resp. $\mathrm{Gal}(K_{E',n}/K)$). Furthermore, let $\rho_n : \mathrm{Gal}(K_{E,n}/K) \to GL_2(\mathbb{Z}/n\mathbb{Z})$ (resp. $\rho'_n : \mathrm{Gal}(K_{E',n}/K) \to GL_2(\mathbb{Z}/n\mathbb{Z})$) be the injective homomorphism as given in Theorem 2.3. Then it is clear that $\mathrm{ord}(\rho_n(\sigma_E)) = \mathrm{ord}(-\rho'_n(\sigma_{E'}))$ since both have the same characteristic polynomial $T^2 - a_E T + q \equiv 0 \pmod n$.

Suppose that $2 \nmid d$. We have that $\rho_n(\sigma_E)^d = -I_2^d \rho'_n(\sigma_{E'})^d = I_2$ where I_2 is the identity matrix. By hypothesis, $\rho'_n(\sigma_{E'})^d = -I_2$, and so $\mathrm{ord}(\rho'_n(\sigma_{E'})) = 2d$.

We now suppose that $4|d$. Since $2|d$, we have $\rho'_n(\sigma_{E'})^d = I_2$. So $d'|d$. Suppose that $d' < d$. If d' is even, then $-I_2^{d'} \rho'_n(\sigma_{E'})^{d'} = I_2$, but this implies that $\mathrm{ord}(\rho_n(\sigma_E)) = d'$, a contradiction. If d' is odd then $\rho_n(\sigma_E)^{d'} = -I_2$. But this gives a contradiction since $\rho_n(\sigma_E)^{2d'} = I_2$, but $4 \nmid 2d'$.

Now consider the case that $2|d$, but $4 \nmid d$. Again, we have $\rho'_n(\sigma_{E'})^d = I_2$. So, $d'|d$. If d' is even, then $\rho_n(\sigma_E)^{d'} = I_2$, and so $d|d'$, which implies that $d = d'$. On the other hand, if d' is odd, $\rho_n(\sigma_E)^{d'} = -I_2$. But then $2d' = d$. So we have two possibilities, $d' = d$ or $\frac{d}{2}$.

We show how the parity of $\mathrm{ord}(q,n)$ can distinguish between the two possibilities. We make use of the fact that $\mathrm{ord}(q,n)$ divides both d and d' by Corollary 3.3. Suppose that $\mathrm{ord}(q,n) \equiv 0 \pmod 2$. Then $2|d'$ and $2|d$. We know that $2|d$ (by hypothesis) and we saw that if $2|d'$, then $d' = d$. If $\mathrm{ord}(q,n) \equiv 1 \pmod 2$ then we observe that $\mathrm{ord}(q,n)|\frac{d}{2}$. We also note that both matrices $\rho_n(\sigma_E)$ and $\rho'_n(\sigma_{E'})$ have determinant $\equiv q \pmod n$. In particular, $\det(\rho_n(\sigma_E)^{\frac{d}{2}}) \equiv 1 \pmod n$. Since $\rho_n(\sigma_E)^d = I_2$, we can deduce that $\rho_n(\sigma_E)^{\frac{d}{2}} \sim I_2$ or $\sim -I_2$. But $\rho_n(\sigma_E)^{\frac{d}{2}} \not\sim I_2$ since $d = \mathrm{ord}(\rho_n(\sigma_E))$, so $\rho_n(\sigma_E)^{\frac{d}{2}} \sim -I_2$, which implies that $d' = \frac{d}{2}$. □

7. An application to the modular curve $X(n)/\mathbb{F}_q$

In this section we sketch out how we can use Algorithm 5.2 to count the number of $\mathbb{F}_q$-rational points on the modular curve $X(n)/\mathbb{F}_q$ when $q \equiv 1 \pmod n$. The material of this section allows us to partially verify our algorithm for the special cases of $n = 3$ and $n = 5$, and $q = p$ when $p \equiv 1 \pmod n$.

For this section we are appealing to the theory concerning the modular curve $X(n)$ (cf. [6] [3]). For this entire discussion we assume the following conditions hold: first, $n \neq \mathrm{char}(K) = p$ is an odd prime and $p \neq 2, 3$, and secondly, $K = \mathbb{F}_q$ contains all the n^{th} roots of unity $\zeta_n \in K$, or equivalently, $q \equiv 1 \pmod n$.

The curve $X(n)$ is a smooth, geometrically irreducible, projective curve over the field K. We now let $Y(n) = X(n) \backslash \text{cusps}$, where the cusps are K-rational points. Then, for any $K' \supset K$, the K'-rational points of $Y(n)$ can be interpreted in terms of 3-tuples $(E, P, Q)_{/K'}$. Here E is an elliptic curve over K', and $P, Q \in E(\overline{K})$ are K'-rational points which form a basis for $E[n]$.

For any extension $K' \supset K$, there exists [6] a natural bijection between the points $x \in Y(n)(K')$ and the isomorphism classes of 3-tuples, i.e., $Y(n)(K') \longleftrightarrow \text{Iso. Classes}(E, P, Q)_{/K'}$. In other words, we identify each $y \in Y(n)(K')$ with a 3-tuple $(E, P, Q)_{/K'}$, where $(E, P, Q)_{/K'}$ is a representative of its isomorphism class.

The group $G_n = Sl_2(\mathbb{Z}/n\mathbb{Z})/\pm 1$ naturally acts on $X(n)$ and on $Y(n)$ via the the above bijection as follows:

$$M \cdot (E, P, Q) = (E, aP + cQ, bP + dQ)$$

where $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_n$. In addition there is a G_n-equivariant morphism $f : X(n) \to X(1) \cong \mathbb{P}^1_K$ defined by $(E, P, Q) \mapsto j_E$ and cusps $\mapsto \infty$, such that $G_n \backslash X(n) \cong X(1)$. In other words, the point $x = (E, P, Q)$ is taken to the j-invariant of the elliptic curve E and the cusps of $X(n)$, which are K-rational, are taken to ∞, the point at infinity of $\mathbb{P}^1_K$.

Since G_n acts faithfully we have

$$\deg(f) = |SL_2(\mathbb{Z}/n\mathbb{Z})/\pm 1| = \frac{n(n^2-1)}{2}. \tag{3}$$

Moreover, if $K(X(n))$ and $K(X(1))$ are the functions field of $X(n)$ and $X(1)$ respectively, then it can be shown that $K(X(n))^{G_n} = K(X(1))$. Since $K(X(n))/K(X(1))$ is Galois [6], the ramification index $e_x(f)$ of $f : X(n) \to X(1)$ and $x \in X(n)$ depends only on $f(x) = y$, so we can write $e_y = e_x(f)$. From [6], if $\mathrm{char}(K) \neq 2, 3$, we have

$$e_y = \begin{cases} n & \text{if } y = \infty \\ 3 & \text{if } y = 0 \\ 2 & \text{if } y = 1728 \end{cases}$$

where $e_y = 1$ otherwise.

We note that for every tuple $(E, P, Q)_{/K}$ that since $P, Q \in E(K)$, then $E[n] \subset E(K)$, thereby implying $[K_{E,n} : K] = 1$. In particular, if $(E, P, Q) \in X(n)(K)$, then $[K_{E,n} : K] = 1$. Conversely, if E is an elliptic curve with $[K_{E,n} : K] = 1$, then E gives rise to to precisely $\frac{deg(f)}{e_{j_E}}$ rational points on $X(n)$. Thus, this gives us the following result:

Proposition 7.1. *Let $K = \mathbb{F}_q$, $n \neq \mathrm{char}(K) = p$ is an odd prime, $p \neq 2, 3$ and $q \equiv 1 \pmod{n}$. Then*

$$\#X(n)(\mathbb{F}_q) \quad = \quad \frac{\deg(f)}{e_\infty} + c_0 \frac{\deg(f)}{e_0} + c_{1728} \frac{\deg(f)}{e_{1728}} + c \deg(f)$$

where

$$\begin{aligned} c_0 &= \#\{E/\mathbb{F}_q \mid [K_{E,n} : K] = 1 \text{ and } j_E = 0\}, \\ c_{1728} &= \#\{E/\mathbb{F}_q \mid [K_{E,n} : K] = 1 \text{ and } j_E = 1728\}, \\ c &= \#\{E/\mathbb{F}_q \mid [K_{E,n} : K] = 1 \text{ and } j_E \neq 0, 1728\}. \end{aligned}$$

Our algorithm enables us to compute the values of c_{1728}, c_0, and c, thus giving us a means to compute $\#X(n)(\mathbb{F}_q)$. As an application, we can compute some of the coefficients of the zeta function of $X(n)/\mathbb{F}_q$. Recall that

$$Z_{X(n)/\mathbb{F}_q}(T) = \exp\left(\sum_{i=1}^{\infty} \frac{\#X(n)(\mathbb{F}_{q^i})}{i} T^i \right).$$

Since $Z_{X(n)/\mathbb{F}_q}(T)$ is a rational function, we need to compute only finitely many $\#X(n)(\mathbb{F}_{q^i})$ to determine *all* the coefficients. However, there is a question of whether this is a practical approach since the implementation of our algorithm

prime p	c_0	c_{1728}	c	$\#X(3)(\mathbb{F}_p)$
7	1	0	0	8
13	1	1	0	14
19	1	0	1	20
31	1	0	2	32
37	1	1	2	38
43	1	0	3	44
61	1	1	4	62
67	1	0	5	68
73	1	1	5	74
79	1	0	6	80
97	1	1	7	98

TABLE 1. Comparing the Output of the Algorithm to $\#X(3)(\mathbb{F}_p)$

prime p	c_0	c_{1728}	c	$\#X(5)(\mathbb{F}_p)$
11	0	0	0	12
31	1	0	0	32
41	0	1	0	42
61	1	1	0	62
71	0	0	1	72

TABLE 2. Comparing the Output of the Algorithm to $\#X(5)(\mathbb{F}_p)$

requires the arithmetic of $\mathbb{F}_q$. In our implementation, we chose to consider only the case when $q = p$.

We conclude by specializing to the case that $n = 3$ and $n = 5$ and consider $X(n)_{/K}$ where $K = \mathbb{F}_q$ and $q \equiv 1 \pmod{n}$. The above discussion allows us to check our tables in a limited sense. We need the following formula that computes the genus of $X(n)$:

$$2g(X(n)) - 2 = \deg(f) \left(2g(X(1)) - 2 + \sum_{y \in X(1)} (1 - \frac{1}{e_y}) \right). \tag{4}$$

Here, $g(X(n))$ and $g(X(1))$ refer to the genus of $X(n)$ and $X(1)$ respectively (see [5] IV.2.4). Since $X(1)_{/K} \cong \mathbb{P}^1_K$, we know that $g(X(1)) = 0$. We compute the genus of $X(3)$ and $X(5)$ and find that $g(X(3)) = g(X(5)) = 0$. So, $X(n) \cong \mathbb{P}^1_K$ for $n = 3, 5$. We deduce that $\#X(n)(\mathbb{F}_q) = q + 1$ for both $n = 3, 5$.

For $n = 3$, we used our algorithm and Proposition 7.1 to compute $\#X(n)(\mathbb{F}_p)$ for all primes $p < 100$ and $p \equiv 1 \pmod{3}$. Comparing this to the expected result of $p + 1$, we see that in all cases they agree. Table 1 contains our results for this comparison. The first column contains all primes $p < 100$ such that $p \equiv 1 \pmod{3}$. Columns two through four contain the values of c_0, c_{1728}, and c that were obtained via our algorithm. In the last column, we use our observed data to evaluate $\#X(3)(\mathbb{F}_p)$.

The case $n = 5$ is very similar. The only difference is that we must use $p \equiv 1 \pmod{5}$. The observed results again agree with the expected results for all $p < 100$. We include a table (Table 2) for this situation.

8. Tables

We include three tables to give a flavor of the output of Algorithm 5.2. The tables contain all elliptic curves over $K = \mathbb{F}_p$ for $p = 7, 11$, and 19, and calculates the field of n-torsion points for all primes $3 \leq n \leq 19$. For each p, we constructed all elliptic curves over the field K as described in Section 6. In the tables, the first four columns correspond to the following information about the elliptic curves:

(*i*) j is the j-invariant of the curve. We write 1728 if $j \equiv 1728 \pmod{p}$.
(*ii*) a and b are the coefficients of the Weierstrass equation for E, that is, $E : y^2 = x^3 + ax + b$.
(*iii*) $a_p = (p+1) - \#E(\mathbb{F}_p)$. From this column, we can also deduce $\#E(\mathbb{F}_p)$.

The remaining columns give the value of d_n, where $d_n = [K_{E,n} : K]$, and n is a prime $3 \leq n \leq 19$. Reading across the table, we get an elliptic curve and the value of d_n for this curve for various n. The row at the end of each table contains the $\mathrm{ord}(p, n)$, that is, the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$.

The tables were generated using Algorithm 5.2 implemented in Maple V Release 4.

j	a	b	a_p	d_3	d_5	d_7	d_{11}	d_{13}	d_{17}	d_{19}
0	0	1	-4	3	24	-	120	12	288	18
0	0	2	-1	1	24	-	120	12	288	18
0	0	3	-5	6	8	-	40	12	288	9
0	0	4	5	3	8	-	40	12	288	18
0	0	5	1	2	24	-	120	12	288	9
0	0	6	4	6	24	-	120	12	288	9
1	4	6	-3	4	4	-	10	168	16	114
1	1	1	3	4	4	-	10	168	16	57
2	3	1	-4	3	24	-	120	12	288	18
2	6	6	4	6	24	-	120	12	288	9
3	6	2	-1	3	24	-	120	12	288	18
3	5	5	1	6	24	-	120	12	288	9
4	5	4	-2	6	4	-	10	168	96	30
4	3	3	2	3	4	-	10	168	96	15
5	2	3	2	3	4	-	10	168	96	15
5	4	4	-2	6	4	-	10	168	96	30
1728	1	0	0	4	8	-	10	24	32	12
1728	3	0	0	4	8	-	10	24	32	12
$\mathrm{ord}(p, n)$				1	4	-	10	12	16	3

Table 3. Elliptic curves over $\mathbb{F}_p$, where $p = 7$

j	a	b	a_p	d_3	d_5	d_7	d_{11}	d_{13}	d_{17}	d_{19}
0	0	1	0	2	4	12	-	24	32	12
0	0	2	0	2	4	12	-	24	32	12
1728	1	0	0	2	4	12	-	24	32	12
1728	2	0	0	2	4	12	-	24	32	12
2	1	9	4	8	3	21	-	168	96	60
2	4	6	-4	8	6	42	-	168	96	60
3	9	4	-6	2	3	24	-	168	16	18
3	3	10	6	2	6	24	-	168	16	9
4	8	6	3	2	10	42	-	12	16	15
4	10	4	-3	2	5	21	-	12	16	30
5	2	7	5	8	4	3	-	168	16	114
5	8	1	-5	8	4	6	-	168	16	57
6	5	1	1	8	6	24	-	12	16	60
6	9	8	-1	8	3	24	-	12	16	60
7	7	8	-2	8	10	3	-	12	288	18
7	6	9	2	8	5	6	-	12	288	9
8	10	2	4	8	3	21	-	168	96	60
8	7	5	-4	8	6	42	-	168	96	60
9	4	3	-2	8	10	3	-	12	288	18
9	5	2	2	8	5	6	-	12	288	9
10	3	5	3	2	10	42	-	12	16	15
10	1	7	-3	2	5	21	-	12	16	30
ord(p, n)				2	1	3	-	12	16	3

TABLE 4. Elliptic curves over $\mathbb{F}_p$, where $p = 11$

j	a	b	a_p	d_3	d_5	d_7	d_{11}	d_{13}	d_{17}	d_{19}
0	0	1	8	3	12	6	120	12	144	-
0	0	2	7	2	12	6	40	12	144	-
0	0	4	-1	3	4	6	120	12	144	-
0	0	5	-7	1	12	6	40	12	144	-
0	0	8	-8	6	12	6	120	12	144	-
0	0	10	1	6	4	6	120	12	144	-
1	15	8	2	1	12	48	10	168	16	-
1	3	7	-2	2	12	48	10	168	16	-
2	1	17	-8	6	12	6	120	12	144	-
2	4	3	8	3	12	6	120	12	144	-
3	13	12	7	6	12	6	40	12	144	-
3	14	1	-7	3	12	6	40	12	144	-
4	5	9	1	6	20	6	120	12	144	-
4	1	15	-1	3	20	6	120	12	144	-
5	6	7	4	6	20	48	40	168	8	-
5	5	18	-4	3	20	48	40	168	8	-
6	4	11	-1	3	20	6	120	12	144	-
6	16	12	1	6	20	6	120	12	144	-
7	12	14	0	4	2	6	10	24	16	-
7	10	17	0	4	2	6	10	24	16	-
8	14	10	3	4	12	48	120	168	8	-
8	18	4	-3	4	12	48	120	168	8	-
9	8	3	-4	3	20	48	40	168	8	-
9	13	5	4	6	20	48	40	168	8	-
10	10	18	5	3	2	48	10	12	272	-
10	2	11	-5	6	2	48	10	12	272	-
11	18	2	6	4	20	6	10	12	48	-
11	15	16	-6	4	20	6	10	12	48	-
12	16	6	-6	4	20	6	10	12	48	-
12	7	10	6	4	20	6	10	12	48	-
13	17	4	2	3	12	48	10	168	16	-
13	11	13	-2	6	12	48	10	168	16	-
14	9	1	2	3	12	48	10	168	16	-
14	17	8	-2	6	12	48	10	168	16	-
15	2	15	4	6	20	48	40	168	8	-
15	8	6	-4	3	20	48	40	168	8	-
16	7	5	5	3	2	48	10	12	272	-
16	9	2	-5	6	2	48	10	12	272	-
17	3	13	-4	3	20	48	40	168	8	-
17	12	9	4	6	20	48	40	168	8	-
1728	1	0	0	4	2	6	10	24	16	-
1728	2	0	0	4	2	6	10	24	16	-
$\mathrm{ord}(p,n)$				1	2	6	10	12	8	-

TABLE 5. Elliptic curves over $\mathbb{F}_p$, where $p = 19$

References

[1] A.O.L. Atkin, Public email messages. (1990-1992).

[2] Ian Blake, Gadiel Seroussi, Nigel Smart, *Elliptic Curves in Cryptography*. London Math. Soc. LNS 256, Cambridge University Press (1999).

[3] Pierre Deligne, Formes Modulaires et Représentations l-adiques, Seminaire Bourbaki, no. 355. (1968/69).

[4] Noam D. Elkies, Elliptic and modular curves over finite fields and related computational issues, in *Computational perspectives on number theory (Chicago, IL, 1995)*. AMS/IP Stud. Adv. Math., 7, Amer. Math. Soc., Providence, RI. (1998) 21-76.

[5] Robin Hartshorne, *Algebraic Geometry*. Springer-Verlag: New York (1977).

[6] Jun-ichi Igusa, Fibre systems of Jacobian varieties III. (Fibre systems of elliptic curves). *Amer. J. Math.* **81** (1959) 453-476.

[7] Serge Lang, *Elliptic Functions*. Addison-Wesley (1973).

[8] Serge Lang, *Elliptic Curves: Diophantine Analysis*. Springer-Verlag (1983).

[9] Rene Schoof, Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.* **44** (1985) 483-494.

[10] Rene Schoof, Counting Points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux* **7** (1995) 219-254.

[11] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. Springer-Verlag: New York (1986).

[12] John Tate, The Arithmetic of Elliptic Curves. *Invent. Math.* **23** (1974), 179-206.

[13] Andrew Wiles, Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)* **141** (1995) 443–551.

Department of Mathematics and Statistics, Queen's University, Kingston, ON K7L 3N6, Canada

E-mail address: vantuyl@mast.queensu.ca